

Five Constructions of Permutation Polynomials over $\text{GF}(q^2)$

Cunsheng Ding^a, Pingzhi Yuan^b

^aDepartment of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China

^bSchool of Mathematics, South China Normal University, Guangzhou 510631, China

Abstract

Four recursive constructions of permutation polynomials over $\text{GF}(q^2)$ with those over $\text{GF}(q)$ are developed and applied to a few famous classes of permutation polynomials. They produce infinitely many new permutation polynomials over $\text{GF}(q^{2^\ell})$ for any positive integer ℓ with any given permutation polynomial over $\text{GF}(q)$. A generic construction of permutation polynomials over $\text{GF}(2^{2m})$ with o-polynomials over $\text{GF}(2^m)$ is also presented, and a number of new classes of permutation polynomials over $\text{GF}(2^{2m})$ are obtained.

Keywords: Hyperoval, permutation polynomials, o-polynomials.

1. Introduction

It is well known that every function from $\text{GF}(q)$ to $\text{GF}(q)$ can be expressed as a polynomial over $\text{GF}(q)$. A polynomial $f \in \text{GF}(q)[x]$ is called a *permutation polynomial* (PP) if the associated polynomial function $f : a \mapsto f(a)$ from $\text{GF}(q)$ to $\text{GF}(q)$ is a permutation of $\text{GF}(q)$.

Permutation polynomials have been a hot topic of study for many years, and have applications in coding theory [15, 28], cryptography [16, 17, 20, 24, 23], combinatorial designs [9], and other areas of mathematics and engineering. Permutation polynomials could have a huge impact in both theory and applications. For instance, the Dickson permutation polynomials of order five over $\text{GF}(3^m)$, i.e., $D_5(x, a) = x^5 + ax^3 - a^2x$, led to a 70-year research breakthrough in combinatorics [9], gave a family of perfect nonlinear functions for cryptography [9], generated good linear codes [3, 31] for data communication and storage, and produced optimal signal sets for CDMA communications [8], to mention only a few applications of these permutation polynomials. A lot of progress on permutation polynomials has been made recently (see, for example, [1, 2, 12, 13, 14, 29, 30, 32], and the references therein).

The objective of this paper is to present five constructions of permutation polynomials over $\text{GF}(q^2)$ with those over $\text{GF}(q)$. Four of them are recursive constructions, so that a sequence of permutation polynomials over $\text{GF}(q^{2^\ell})$ can be constructed with only one permutation polynomial over $\text{GF}(q)$, where ℓ is any positive integer. Another construction of permutation polynomials over $\text{GF}(2^{2m})$ with o-polynomials over $\text{GF}(2^m)$ is also developed. This nonrecursive construction

^{*}C. Ding's research was supported by The Hong Kong Research Grants Council, Proj. No. 601013. P. Yuan's research was supported by the NSF of China (Grant No. 11271142).

Email addresses: cding@ust.hk (Cunsheng Ding), mcsypz@mail.sysu.edu.cn (Pingzhi Yuan)

Preprint submitted to Elsevier

November 12, 2015

gives several classes of new permutation polynomials over $\text{GF}(2^{2m})$ with known classes of o-polynomials over $\text{GF}(2^m)$.

2. Some preparations

Before presenting the five constructions of PPs over $\text{GF}(q^2)$ from those over $\text{GF}(q)$, we need to prove a few basic results as a preparation for subsequent sections.

2.1. A general theorem about permutation polynomials

The following is a fundamental result of this paper.

Theorem 1. *Let $\{\beta_1, \dots, \beta_m\}$ and $\{\gamma_1, \dots, \gamma_m\}$ be two bases of $\text{GF}(q^m)$ over $\text{GF}(q)$. Let A be an $m \times m$ nonsingular matrix over $\text{GF}(q)$ and $f_i(x) \in \text{GF}(q)[x]$ for $i = 1, \dots, m$. Then*

$$F(z) = \gamma_1 f_1(x_1) + \dots + \gamma_m f_m(x_m),$$

where $(x_1, \dots, x_m) = (z_1, \dots, z_m)A$ and $z = \beta_1 z_1 + \dots + \beta_m z_m$, is a PP over $\text{GF}(q^m)$ if and only if all $f_i(x), i = 1, \dots, m$, are PPs over $\text{GF}(q)$.

Proof. We first prove the sufficiency of the conditions and assume now that all $f_i(x), i = 1, \dots, m$, are PPs over $\text{GF}(q)$. Let

$$z = \beta_1 z_1 + \dots + \beta_m z_m, \quad y = \beta_1 y_1 + \dots + \beta_m y_m, \quad z_i, y_i \in \text{GF}(q),$$

be two elements of $\text{GF}(q^m)$ such that $F(z) = F(y)$. Let

$$(x_1, \dots, x_m) = (z_1, \dots, z_m)A$$

and

$$(u_1, \dots, u_m) = (y_1, \dots, y_m)A.$$

Then

$$\gamma_1 f_1(x_1) + \dots + \gamma_m f_m(x_m) = \gamma_1 f_1(u_1) + \dots + \gamma_m f_m(u_m).$$

Since $\{\gamma_1, \dots, \gamma_m\}$ is a basis of $\text{GF}(q^m)$ over $\text{GF}(q)$, we deduce that $f_i(x_i) = f_i(u_i)$ for $i = 1, \dots, m$. Note that all $f_i(x), i = 1, \dots, m$, are PPs over $\text{GF}(q)$. We obtain that $x_i = u_i$, and thus $z_i = y_i$, as A is an $m \times m$ nonsingular matrix over $\text{GF}(q)$. Therefore $z = y$, and hence $F(z)$ is a PP over $\text{GF}(q^m)$.

We now prove the necessity of the conditions, and assume that $F(z)$ is a PP over $\text{GF}(q^m)$. Suppose on the contrary that some $f_i(x)$ is not PP over $\text{GF}(q)$. Without loss of generality, we may assume that $f_1(x)$ is not a PP over $\text{GF}(q)$. Then there exist two distinct elements $x_1, u_1 \in \text{GF}(q)$ such that $x_1 \neq u_1$ and $f_1(x_1) = f_1(u_1)$. Let

$$(y_1, \dots, y_m) = (u_1, 0, \dots, 0)A^{-1}, \quad (z_1, \dots, z_m) = (x_1, 0, \dots, 0)A^{-1}.$$

Then $(y_1, \dots, y_m) \neq (z_1, \dots, z_m)$ and $y \neq z$, since A is an $m \times m$ nonsingular matrix over $\text{GF}(q)$. Hence $F(z) = F(y)$ with $y \neq z$, which contradicts to our assumption that $F(z)$ is a PP over $\text{GF}(q^m)$. \square

2.2. $\text{GF}(q^2)$ as a two-dimensional space over $\text{GF}(q)$

In this subsection, we represent every element of $\text{GF}(q^2)$ as a pair of elements in $\text{GF}(q)$ with respect to a basis of $\text{GF}(q^2)$ over $\text{GF}(q)$.

Let $r = q^2$, where q is a power of a prime. Let β be a generator of $\text{GF}(r)$. Then $\{1, \beta\}$ is a basis of $\text{GF}(r)$ over $\text{GF}(q)$, and any element $z \in \text{GF}(r)$ can be expressed as

$$z = x + y\beta,$$

where

$$x = \frac{\beta^q z - \beta z^q}{\beta^q - \beta} \in \text{GF}(q), \quad y = \frac{z^q - z}{\beta^q - \beta} \in \text{GF}(q). \quad (1)$$

3. A construction of permutation polynomials over $\text{GF}(q^2)$ with o-polynomials over $\text{GF}(q)$

Throughout this section, let $q = 2^m$, where $m > 1$ is a positive integer. A permutation polynomial f on $\text{GF}(q)$ is called an *o-polynomial* if $f(0) = 0$, and for each $s \in \text{GF}(q)$,

$$f_s(x) = (f(x+s) + f(s))x^{q-2} \quad (2)$$

is a permutation polynomial. In the original definition of o-polynomials, it is required that $f(1) = 1$. However, this is not essential, as one can always normalise $f(x)$ by using $f(1)^{-1}f(x)$ due to that $f(1) \neq 0$.

A *hyperoval* of the projective plane $\text{PG}(2, q)$ is a set of $q+2$ points such that no three of them are collinear. Any hyperoval in $\text{PG}(2, q)$ can be written as

$$O_f = \{(1, t, f(t)) : t \in \text{GF}(q)\} \cup \{(0, 1, 0), (0, 0, 1)\} \quad (3)$$

where f is a o-polynomial over $\text{GF}(q)$ with $f(0) = 0$ and $f(1) = 1$. Two o-polynomials are called *equivalent* if their hyperovals are equivalent.

In this section, we will present a construction of PPs over $\text{GF}(q^2)$ with o-polynomials over $\text{GF}(q)$ and will give a summary of known o-polynomials over $\text{GF}(q)$.

3.1. The construction

Let f be a polynomial over $\text{GF}(q)$ and let β be a generator of $\text{GF}(q^2)^*$. We now define a polynomial $F(z)$ over $\text{GF}(q^2)$ by

$$\begin{aligned} F(z) &= xf(yx^{q-2}) + \beta y + ((z + z^q)^{q-1} + 1)z \\ &= \frac{\beta^q z + \beta z^q}{\beta^q + \beta} f\left[\left(\frac{\beta^q z + \beta z^q}{\beta^q + \beta}\right) \left(\frac{z + z^q}{\beta^q + \beta}\right)^{q-2}\right] + ((z + z^q)^{q-1} + 1)z, \end{aligned} \quad (4)$$

where $z = x + \beta y$, $x \in \text{GF}(q)$, $y \in \text{GF}(q)$ and z are also related by the expression of (1).

Theorem 2. *If f is an o-polynomial over $\text{GF}(q)$, then the polynomial $F(x)$ of (4) is a PP over $\text{GF}(q^2)$.*

Proof. Since $z + z^q = (\beta + \beta^q)y \in \text{GF}(q)$ and $z + z^q = 0$ if and only if $y = 0$, so $(z + z^q)^{q-1} = 1$ when $y \neq 0$ and 0 otherwise. Hence $F(z) = xf(yx^{q-2}) + \beta y$ when $y \neq 0$, and $F(z) = x$ when $y = 0$.

Let $z_1 = x_1 + \beta y_1$ and $z_2 = x_2 + \beta y_2$. Assume that $F(z_1) = F(z_2)$. We first consider the case that $y_1 = 0$ and $y_2 = 0$. In this case, we have

$$F(z_1) = x_1 = x_2 = F(z_2).$$

Hence $x_1 = x_2$, and then $z_1 = z_2$. Therefore we may assume that $y_1 \neq 0$. In this case, we have

$$F(z_1) = x_1 f(y_1 x_1^{q-2}) + \beta y_1 = F(z_2) = x_2 f(y_2 x_2^{q-2}) + \beta y_2.$$

Hence $y_2 \neq 0$ and $y_1 = y_2 = y$ since $\{1, \beta\}$ is a basis of $\text{GF}(q^2)$ over $\text{GF}(q)$. It follows that

$$x_1 f(y x_1^{q-2}) = x_2 f(y x_2^{q-2}). \quad (5)$$

Since f is an o-polynomial over $\text{GF}(q)$, by definition, $f_0(x) := f(x)x^{q-2}$ is a permutation polynomial over $\text{GF}(q)$. Note that yx^{q-2} is also a permutation polynomial over $\text{GF}(q)$, which implies that $f_0(yx^{q-2}) = y^{q-2}xf(yx^{q-2})$ is a permutation polynomial over $\text{GF}(q)$. Hence $xf(yx^{q-2})$ is a permutation polynomial over $\text{GF}(q)$. It follows from (5) that $x_1 = x_2$, and so $z_1 = z_2$. This proves the theorem. \square

In the construction of this section, the o-polynomial property of $f(x)$ is sufficient. But it is open if it is necessary.

3.2. Known o-polynomials over $\text{GF}(2^m)$

To obtain permutation polynomials over $\text{GF}(2^{2m})$ with the generic construction of Section 3.1, we need explicit o-polynomials over $\text{GF}(2^m)$ as building blocks. O-polynomials have many special properties. For instance, the coefficient of each term of odd power in an o-polynomial is zero [21].

In this subsection, we summarize and extend known o-polynomials over $\text{GF}(2^m)$. We also introduce some basic results about o-polynomials.

3.2.1. Basic properties of o-polynomials

For any permutation polynomial $f(x)$ over $\text{GF}(2^m)$, we define $\bar{f}(x) = xf(x^{2^m-2})$, and use f^{-1} to denote the compositional inverse of f , i.e., $f^{-1}(f(x)) = x$ for all $x \in \text{GF}(2^m)$.

The following theorem introduces basic properties of o-polynomials whose proofs are easy [21].

Theorem 3. *Let f be an o-polynomial on $\text{GF}(2^m)$. Then the following holds:*

- a) f^{-1} is also an o-polynomial;
- b) $f(x^{2^j})^{2^{m-j}}$ is also an o-polynomial for any $1 \leq j \leq m-1$;
- c) \bar{f} is also an o-polynomial; and
- d) $f(x+1) + f(1)$ is also an o-polynomial.

Although these o-polynomials are equivalent to the original o-polynomial f in terms of their hyperovals, they may produce different objects when they are used in other applications.

All o-monomials are characterised by the following theorem [11, Corollary 8.2.4].

Theorem 4. *The monomial x^k is an o-polynomial over $\text{GF}(2^m)$ if and only if*

- a) $\gcd(k, 2^m - 1) = 1$;
- b) $\gcd(k - 1, 2^m - 2) = 1$; and
- c) $((x + 1)^k + 1)x^{2^m - 2}$ is a permutation polynomial over $\text{GF}(2^m)$.

For o-monomials we have the following fundamental result [11].

Theorem 5. *Let x^k be an o-polynomial on $\text{GF}(2^m)$. Then every polynomial in*

$$\left\{ x^{\frac{1}{k}}, x^{1-k}, x^{\frac{1}{1-k}}, x^{\frac{k}{k-1}}, x^{\frac{k-1}{k}} \right\}$$

is also an o-monomial, where $1/k$ denotes the multiplicative inverse of k modulo $2^m - 1$.

3.2.2. The translation o-polynomials

The translation o-polynomials are described in the following theorem [25].

Theorem 6. *$\text{Trans}(x) = x^{2^h}$ is an o-polynomial on $\text{GF}(2^m)$, where $\gcd(h, m) = 1$.*

The following is a list of known properties of translation o-polynomials.

- 1) $\text{Trans}^{-1}(x) = x^{2^{m-h}}$ and
- 2) $\overline{\text{Trans}}(x) = xf(x^{2^m - 2}) = x^{2^m - 2^{m-h}}$.

3.2.3. The Segre and Glynn o-polynomials

The following theorem describes a class of o-polynomials, which are an extension of the original Segre o-polynomials.

Theorem 7. *Let m be odd. Then $\text{Segre}_a(x) = x^6 + ax^4 + a^2x^2$ is an o-polynomial on $\text{GF}(2^m)$ for every $a \in \text{GF}(2^m)$.*

Proof. The conclusion follows from

$$\text{Segre}_a(x) = (x + \sqrt{a})^6 + \sqrt{a}^3.$$

□

We have the following remarks on this family of o-polynomials.

- a) $\text{Segre}_0(x) = x^6$ is the original Segre o-polynomial [26, 27]. So this is an extended family.
- b) $\text{Segre}_a(x) = xD_5(x, a) = a^2D_5(x^{2^m - 2}, a^{2^m - 2})x^7$, where $D_5(x, a) = x^5 + ax^3 + a^2x$, which is the Dickson polynomial of the first kind of order 5 [18].
- c) $\overline{\text{Segre}}_a = D_5(x^{2^m - 2}, a) = a^2x^{2^m - 2} + ax^{2^m - 4} + x^{2^m - 6}$.
- d) $\text{Segre}_a^{-1}(x) = (x + \sqrt{a}^3)^{\frac{5 \times 2^{m-1} - 2}{3}} + \sqrt{a}$.

The proof of the following theorem is straightforward and omitted.

Theorem 8. *Let m be odd. Then*

$$\overline{\text{Segre}}_1^{-1}(x) = \left(D_{\frac{3 \times 2^{m-2}}{5}}(x, 1) \right)^{2^m - 2}. \quad (6)$$

Glynn discovered two families of o-polynomials [10]. The first is described as follows.

Theorem 9. *Let m be odd. Then $\text{Glynni}(x) = x^{3 \times 2^{(m+1)/2} + 4}$ is an o-polynomial.*

An extension of the second family of o-polynomials discovered by Glynn is documented in the following theorem.

Theorem 10. *Let m be odd. Then*

$$\text{Glynnii}_a(x) = \begin{cases} x^{2^{(m+1)/2} + 2^{(3m+1)/4}} + ax^{2^{(m+1)/2}} + (ax)^{2^{(3m+1)/4}} & \text{if } m \equiv 1 \pmod{4}, \\ x^{2^{(m+1)/2} + 2^{(m+1)/4}} + ax^{2^{(m+1)/2}} + (ax)^{2^{(m+1)/4}} & \text{if } m \equiv 3 \pmod{4}. \end{cases}$$

is an o-polynomial for all $a \in \text{GF}(q)$.

Proof. Let $m \equiv 1 \pmod{4}$. Then

$$\text{Glynnii}_a(x) = (x + a^{(m-1)/4})^{2^{(m+1)/2} + 2^{(3m+1)/4}} + a^{2^{(m+1)/2} + 2^{(3m+1)/4}}.$$

The desired conclusion for the case $m \equiv 1 \pmod{4}$ can be similarly proved. \square

Note that $\text{Glynnii}_0(x)$ is the original Glynn o-polynomial. So this is an extended family. For some applications, the extended family may be useful.

3.2.4. The Cherowitzo o-polynomials

The following describes another class of o-polynomials.

Theorem 11. *Let m be odd and $e = (m+1)/2$. Then*

$$\text{Cherowitzo}_a(x) = x^{2^e} + ax^{2^e+2} + a^{2^e+2}x^{3 \times 2^e+4}$$

is an o-polynomial on $\text{GF}(2^m)$ for every $a \in \text{GF}(2^m)$.

We have the following remarks on this family.

- 1) $\text{Cherowitzo}_1(x)$ is the original Cherowitzo o-polynomial [4, 5]. So this is an extended family.
- 2) A proof of the o-polynomial property of this extended family goes as follows. It can be easily verified that $\text{Cherowitzo}_a(x) = a^{-2^{e-1}} \text{Cherowitzo}_1(a^{1/2}x)$. The desired conclusion then follows.
- 3) $\overline{\text{Cherowitzo}}(x) = x^{2^m-2^e} + ax^{2^m-2^e-2} + a^{2^e+2}x^{2^m-3 \times 2^e-4}$.
- 4) It is known that $\text{Cherowitzo}_1^{-1}(x) = x(x^{2^e+1} + x^3 + x)^{2^{e-1}-1}$.

The proofs of the following two theorems are straightforward and left to the reader.

Theorem 12.

$$\text{Cherowitzo}_a^{-1}(x) = x(ax^{2^e+1} + a^{2^e}x^3 + x)^{2^{e-1}-1}.$$

Theorem 13.

$$\overline{\text{Cherowitzo}} = (ax^{2^m-2^e-2} + a^{2^e}x^{2^m-4} + x^{2^m-2})^{2^{e-1}-1}.$$

3.2.5. The Payne o-polynomials

The following documents an extended family of o-trinomials.

Theorem 14. *Let m be odd. Then $\text{Payne}_a(x) = x^{\frac{5}{6}} + ax^{\frac{3}{6}} + a^2x^{\frac{1}{6}}$ is an o-polynomial on $\text{GF}(2^m)$ for every $a \in \text{GF}(2^m)$, where $\frac{1}{6}$ denotes the multiplicative inverse of 6 modulo $2^m - 1$.*

We have the following remarks on this family.

- a) $\text{Payne}_1(x)$ is the original Payne o-polynomial [22]. So this is an extended family.
- b) It can be verified that $\text{Payne}_a(x) = a^{5/2}\text{Payne}_1(a^{-3}x)$. The desired conclusion of Theorem 14 follows.
- c) $\overline{\text{Payne}}_a(x) = xD_5(x^{\frac{1}{6}}, a)$.
- d) $\overline{\text{Payne}}_a(x) = a^{2^m-3}\text{Payne}_{a^{2^m-2}}(x)$.
- e) Note that

$$\frac{1}{6} = \frac{5 \times 2^{m-1} - 2}{3}.$$

We have then

$$\text{Payne}_a(x) = x^{\frac{2^{m-1}+2}{3}} + ax^{2^{m-1}} + a^2x^{\frac{5 \times 2^{m-1}-2}{3}}.$$

Theorem 15. *Let m be odd. Then*

$$\text{Payne}_1^{-1}(x) = \left(D_{\frac{3 \times 2^{2m}-2}{5}}(x, 1) \right)^6 \quad (7)$$

and $\overline{\text{Payne}}_1^{-1}(x)$ are an o-polynomial.

Proof. Note that the multiplicative inverse of 5 modulo $2^m - 1$ is $\frac{3 \times 2^{2m}-2}{5}$. The conclusion then follows from the definition of the Payne polynomial and the fact that

$$D_5(x, 1)^{-1} = D_{\frac{3 \times 2^{2m}-2}{5}}(x, 1).$$

□

3.2.6. The Subiaco o-polynomials

The Subiaco o-polynomials are given in the following theorem [6].

Theorem 16. *Define*

$$\text{Subiaco}_a(x) = ((a^2(x^4 + x) + a^2(1 + a + a^2)(x^3 + x^2))(x^4 + a^2x^2 + 1)^{2^m-2} + x^{2^{m-1}}),$$

where $\text{Tr}(1/a) = 1$ and $d \notin \text{GF}(4)$ if $m \equiv 2 \pmod{4}$. Then $\text{Subiaco}_a(x)$ is an o-polynomial on $\text{GF}(2^m)$.

As a corollary of Theorem 16, we have the following.

Corollary 17. *Let m be odd. Then*

$$\text{Subiaco}_1(x) = (x + x^2 + x^3 + x^4)(x^4 + x^2 + 1)^{2^m-2} + x^{2^{m-1}} \quad (8)$$

is an o-polynomial over $\text{GF}(2^m)$.

3.2.7. The Adelaide o-polynomials

The last known family of o-polynomials were discovered in [7] and described in the following theorem.

Theorem 18. *Let m be even and $r = q^2$. The trace function from $\text{GF}(r)$ to $\text{GF}(q)$ is defined by $\text{Tr}_2(x) = x + x^q$. Let $b \in \text{GF}(r)$ such that $b^{q+1} = 1$ and $b \neq 1$ and define*

$$\text{Adelaide}_b(x) = \text{Tr}_2(b)^{q-2} \text{Tr}_2(b^\ell)(x+1) + \text{Tr}_2(b)^{q-2} \text{Tr}_2((bx+b^q)^{r_1+\ell})(x + \text{Tr}_2(b)x^{2^{m-1}} + 1)^{q-\ell} + x^{2^{m-1}},$$

where $\ell = \pm(q-1)/3$. Then f_b is an o-polynomial.

We need to clarify the definition of this family of o-polynomials. First of all, $\text{Adelaide}_b(x)$ is defined as a polynomial over $\text{GF}(q)$, while b is an element from the extension field. Secondly, note that ℓ could be negative. The definition above is a modified version of the original one in the literature.

4. The first recursive construction

We now present the first recursive construction of PPs over $\text{GF}(q^2)$ from those over $\text{GF}(q)$. Let $f_1(x)$ and $f_2(x)$ be two polynomials over $\text{GF}(q)$, and let $\beta \in \text{GF}(q^2) \setminus \text{GF}(q)$. Note that $\{1, \beta\}$ is a basis of $\text{GF}(q^2)$ over $\text{GF}(q)$. Let $z = x + \beta y$, where $x \in \text{GF}(q)$, $y \in \text{GF}(q)$ and z are also related by the expression of (1). It follows from Theorem 1 that

$$F_1(z) := f_1(x) + \beta f_2(y) = f_1\left(\frac{\beta^q z - \beta z^q}{\beta^q - \beta}\right) + \beta f_2\left(\frac{z^q - z}{\beta^q - \beta}\right). \quad (9)$$

is a permutation polynomial over $\text{GF}(r)$ if and only if both $f_1(x)$ and $f_2(x)$ are permutation polynomials over $\text{GF}(q)$. This proves the following theorem.

Theorem 19. *Let $f_1(x)$ and $f_2(x)$ be two polynomials over $\text{GF}(q)$. Then the polynomial $F_1(z)$ of (9) is a permutation polynomial over $\text{GF}(q^2)$ if and only if both $f_1(x)$ and $f_2(x)$ are permutation polynomials over $\text{GF}(q)$.*

As a special case of Theorem 19, let $f_1(x) = f_2(x) = f(x)$, where $f(x)$ is a PP over $\text{GF}(q)$. Then this $g(x)$ gives a PP over $\text{GF}(q^2)$, and the newly obtained PP over $\text{GF}(q^2)$ gives another new PP over $\text{GF}(q^4)$. By recursively applying this construction, we obtain a PP over $\text{GF}(q^{2^i})$ for any integer i .

As a demonstration of the generic construction of this section, we consider a few special cases below. We start with the so-called p -polynomials. Let $q = p^m$ for some m . A p -polynomial $L(x)$ over $\text{GF}(q)$ is of the form

$$L(x) = \sum_{i=0}^{\ell-1} l_i x^{p^i},$$

where the coefficients $l_i \in \text{GF}(q)$. It is known that $L(x)$ is a PP over $\text{GF}(q)$ if and only if $L(x)$ has only the root 0 in $\text{GF}(q)$ [19, p. 351]. However, this characterization is not really useful for constructing permutation q -polynomials. The following corollary of Theorem 19 shows that the generic construction of this section can be employed to construct permutation p -polynomials.

Corollary 20. Let $q = p^m$ for some positive integer m . Let $\beta \in \text{GF}(q^2) \setminus \text{GF}(q)$. If $f_1(x)$ and $f_2(x)$ are two permutation p -polynomials over $\text{GF}(q)$, then the polynomial $F_1(z)$ of (9) is a permutation p -polynomial over $\text{GF}(q^2)$.

As a special case of Corollary 20, let

$$f_1(x) = ax^{p^{h_1}} \text{ and } f_2(x) = ax^{p^{h_2}},$$

where $a, b \in \text{GF}(q)^*$ and $0 \leq h_i \leq m-1$ for each i . Then both $f_1(x)$ and $f_2(x)$ are permutation p -polynomials over $\text{GF}(q)$. By Corollary 20,

$$a \left(\frac{\beta^q z - \beta z^q}{\beta^q - \beta} \right)^{p^{h_1}} + \beta b \left(\frac{z^q - z}{\beta^q - \beta} \right)^{p^{h_2}}$$

is a permutation p -polynomial over $\text{GF}(q^2)$.

Note that the monomial ax^u is a PP over $\text{GF}(q)$ if and only if $a \neq 0$ and $\gcd(u, q-1) = 1$. If we choose $f_1(x)$ and $f_2(x)$ in Theorem 19 as monomials, we obtain the following.

Corollary 21. Let $1 \leq u \leq q-1$ and $1 \leq v \leq q-1$ be two integers, and let $\beta \in \text{GF}(q^2) \setminus \text{GF}(q)$. Then

$$\eta \left(\frac{\beta^q z - \beta z^q}{\beta^q - \beta} \right)^u + \gamma \beta \left(\frac{z^q - z}{\beta^q - \beta} \right)^v$$

is a PP over $\text{GF}(q^2)$ if and only if $\gcd(uv, q-1) = 1$, where $\eta \in \text{GF}(q)^*$ and $\gamma \in \text{GF}(q)^*$.

Any PP $f(x)$ over $\text{GF}(q)$ can be plugged into the generic construction of this section to obtain a PP over $\text{GF}(q^2)$. So it is endless to consider all the specific constructions in this paper. However, it would be interesting to investigate the specific permutation polynomials over $\text{GF}(q^2)$ from the Dickson permutation polynomials of the first kind over $\text{GF}(q)$, which are defined by

$$D_h(x, a) = \sum_{i=0}^{\lfloor \frac{h}{2} \rfloor} \frac{h}{h-i} \binom{h-i}{i} (-a)^i x^{h-2i}, \quad (10)$$

where $a \in \text{GF}(q)$ and h is called the *order* of the polynomial. It is known that $D_h(x, a)$ is a PP over $\text{GF}(q)$ if and only if $\gcd(h, q^2-1) = 1$.

As a corollary of Theorem 19, we have the following.

Corollary 22. Let $\beta \in \text{GF}(q^2) \setminus \text{GF}(q)$ and $a \in \text{GF}(q)$. Then the following polynomial

$$\overline{D}_h(x, a) = \sum_{i=0}^{\lfloor \frac{h}{2} \rfloor} \frac{h}{h-i} \binom{h-i}{i} (-a)^i \left[\left(\frac{\beta^q z - \beta z^q}{\beta^q - \beta} \right)^{h-2i} + \beta \left(\frac{z^q - z}{\beta^q - \beta} \right)^{h-2i} \right], \quad (11)$$

is a PP over $\text{GF}(q^2)$ if and only if $\gcd(h, q^2-1) = 1$.

5. The second recursive construction

The second recursive construction is a variant of Theorem 19 and is described below.

Theorem 23. Let $\beta \in \text{GF}(q^2) \setminus \text{GF}(q)$. Let $f_1(x)$ and $f_2(x)$ be two polynomials over $\text{GF}(q)$. Then

$$F_2(z) := f_1\left(\frac{\beta^q z - \beta z^q}{\beta^q - \beta}\right) + \beta f_2\left(\frac{(\beta^q - 1)z - (\beta - 1)z^q}{\beta^q - \beta}\right)$$

is a PP over $\text{GF}(q^2)$ if and only if both $f_1(x)$ and $f_2(x)$ are PPs over $\text{GF}(q)$.

Proof. Let $x_1 = x$ and $x_2 = x + y$. The proof is similar to that of Theorem 19 and is omitted. \square

This is not only a recursive but also a generic construction, into which any permutation polynomials $f_1(x)$ and $f_2(x)$ over $\text{GF}(q)$ can be plugged.

6. The third recursive construction

Let $\beta \in \text{GF}(q^2) \setminus \text{GF}(q)$. Note that $\{\beta + 1, \beta\}$ is also a basis over $\text{GF}(q)$. Let $f_1(x)$ and $f_2(x)$ be two polynomials over $\text{GF}(q)$. We now define a polynomial $F_3(z)$ over $\text{GF}(q^2)$ by

$$\begin{aligned} F_3(z) &= f_1(x) + \beta(f_1(x) + f_2(y)) \\ &= (\beta + 1)f_1\left(\frac{\beta^q z - \beta z^q}{\beta^q - \beta}\right) + \beta f_2\left(\frac{z^q - z}{\beta^q - \beta}\right), \end{aligned} \quad (12)$$

where $z = x + \beta y$, $x \in \text{GF}(q)$, $y \in \text{GF}(q)$ and z are also related by the expression of (1).

The following theorem then follows from Theorem 1.

Theorem 24. Let $\beta \in \text{GF}(q^2) \setminus \text{GF}(q)$, and let $f_1(x)$ and $f_2(x)$ be two polynomials over $\text{GF}(q)$. Then the polynomial $F_3(z)$ of (12) is a PP over $\text{GF}(q^2)$ if and only if both $f_1(x)$ and $f_2(x)$ are PPs over $\text{GF}(q)$.

Example 25. Let q be an odd prime power. Choose an element $b \in \text{GF}(q)$ such that $x^2 - b$ is irreducible over $\text{GF}(q)$. Let β be a solution of $x^2 - b$ in $\text{GF}(q^2)$ (we view $\text{GF}(q^2)$ as the splitting field of $x^2 - b$ over $\text{GF}(q)$). Let

$$x_1 = a_{11}x + 2ba_{12}y \text{ and } x_2 = a_{21}x + 2ba_{22}y,$$

where $a_{11}, a_{12}, a_{21}, a_{22} \in \text{GF}(q)$ with $a_{11}a_{22} - a_{12}a_{21} \neq 0$. Note that $\{1, \beta\}$, $\beta \in \text{GF}(r) \setminus \text{GF}(q)$ is a basis of $\text{GF}(q^2)$ over $\text{GF}(q)$. It then follows from Theorem 1 that

$$((a_{11} + a_{12}\beta)z + (a_{11} - a_{12}\beta)z^q)^u + \alpha((a_{21} + a_{22}\beta)z + (a_{21} - a_{22}\beta)z^q)^v, \alpha \in \text{GF}(r) \setminus \text{GF}(q)$$

is a PP over $\text{GF}(q^2)$ if and only if $\gcd(uv, q-1) = 1$.

7. The fourth recursive construction

Throughout this section, let q be a power of 2 and let $\beta \in \text{GF}(q^2) \setminus \text{GF}(q)$. Let f be a polynomial over $\text{GF}(q)$. We now define a polynomial $G(z)$ over $\text{GF}(q^2)$ by

$$\begin{aligned} G(z) &= f(yx) + \beta y + ((z + z^q)^{q-1} + 1)z \\ &= f\left[\left(\frac{\beta^q z + \beta z^q}{\beta^q + \beta}\right)\left(\frac{z + z^q}{\beta^q + \beta}\right)\right] + ((z + z^q)^{q-1} + 1)z, \end{aligned} \quad (13)$$

where $z = x + \beta y$, $x \in \text{GF}(q)$, $y \in \text{GF}(q)$ and z are also related by the expression of (1).

Theorem 26. *If f is a permutation polynomial over $\text{GF}(q)$, then the polynomial $G(z)$ of (13) is a PP over $\text{GF}(q^2)$.*

Proof. Since q is a power of 2, we have that $z + z^q = (\beta + \beta^q)y \in \text{GF}(q)$. Thus, $z + z^q = 0$ if and only if $y = 0$. It then follows that $(z + z^q)^{q-1} = 1$ when $y \neq 0$ and 0 otherwise. Consequently, $F(z) = f(yx) + \beta y$ when $y \neq 0$ and $F(z) = x$ when $y = 0$.

Let $z_1 = x_1 + \beta y_1$ and $z_2 = x_2 + \beta y_2$. Assume that $F(z_1) = F(z_2)$. We first consider the case that $y_1 = 0$ and $y_2 = 0$. In this case, we have

$$F(z_1) = x_1 = x_2 = F(z_2).$$

Thus, $x_1 = x_2$, and then $z_1 = z_2$. Therefore we may assume that $y_1 \neq 0$. We have

$$F(z_1) = f(y_1 x_1) + \beta y_1 = F(z_2) = f(y_2 x_2) + \beta y_2.$$

As a result, we have $y_2 \neq 0$ and $y_1 = y_2 = y$ since $\{1, \beta\}$ is a basis of $\text{GF}(q^2)$ over $\text{GF}(q)$. It follows that

$$f(yx_1) = f(yx_2). \quad (14)$$

Note that $y \neq 0$. Since $f(x)$ is a permutation polynomial over $\text{GF}(q)$, so is $f(yx)$. It follows from (14) that $x_1 = x_2$. Hence, $z_1 = z_2$. This proves the theorem. \square

Notice that the construction of this section works only for the case that q is a power of 2.

8. Further constructions of permutation polynomials

The generic constructions of permutation polynomials presented in some earlier sections are derived from Theorem 1. In this section, we employ Theorem 1 to get more constructions of permutation polynomials over $\text{GF}(q^2)$ and $\text{GF}(q^3)$.

Theorem 27. *Let q be an odd prime power, t a positive integer, and let $a, b, u \in \text{GF}(q)$. Then*

$$F(z) = az + bz^q + (z + z^q + u)^t$$

is a PP over $\text{GF}(q^2)$ if and only if $a \neq b$ and $(a + b)x + 2x^t$ is a PP over $\text{GF}(q)$.

Proof. Since q is an odd prime power, $2(q - 1)$ must divide $q^2 - 1$. Consequently, there exists an element $\alpha \in \text{GF}(q^2) \setminus \text{GF}(q)$ with $\alpha^q = -\alpha$. Thus $\{1, \alpha\}$ is a basis of $\text{GF}(q^2)$ over $\text{GF}(q)$. Put

$$z = x + y\alpha,$$

then $z^q = x - y\alpha$. It follows that

$$F(z) = (a + b)x + (a - b)y\alpha + (2x + u)^t.$$

By Theorem 1, $F(z)$ is a PP over $\text{GF}(q^2)$ if and only if both $(a - b)x$ and $(a + b)x + (2x + u)^t$ are PPs over $\text{GF}(q)$. It is easily seen that $(a + b)x + (2x + u)^t$ is a PP over $\text{GF}(q)$ if and only if $(a + b)x + 2x^t$ is a PP over $\text{GF}(q)$. The desired conclusions then follow. \square

When $t = 1$, $a \neq b$ and $a + b + 2 \neq 0$, it follows from Theorem 27 that $F(z) = (a + 1)z + (b + 1)z^q + u$ is a PP over $\text{GF}(q^2)$ for any $u \in \text{GF}(q)$.

Theorem 28. Let q be an odd prime power and let t a positive integer. Let $\alpha \in \text{GF}(q^2) \setminus \text{GF}(q)$ with $\alpha^q = -\alpha$ and let $a, b, u \in \text{GF}(q)$.

1. When t is even,

$$F_1(z) = az + bz^q + (z - z^q + u\alpha)^t$$

is a PP over $\text{GF}(q^2)$ if and only if $a^2 \neq b^2$.

2. When t is odd,

$$F_1(z) = az + bz^q + (z - z^q + u\alpha)^t$$

is a PP over $\text{GF}(q^2)$ if and only if $a + b \neq 0$ and $(a - b)x + 2x^t\alpha^{t-1}$ is a PP over $\text{GF}(q)$.

Proof. We first prove the conclusion of the first part. Since $\alpha^q = -\alpha$, $\{1, \alpha\}$ is a basis of $\text{GF}(q^2)$ over $\text{GF}(q)$ and $\alpha^2 \in \text{GF}(q)$. Put

$$z = x + y\alpha,$$

where $x \in \text{GF}(q)$ and $y \in \text{GF}(q)$. Then $z^q = x - y\alpha$. It follows that

$$F_1(z) = (a + b)x + (a - b)y\alpha + (2y + u)^t\alpha^t. \quad (15)$$

If $a + b = 0$, then $F_1(x_1 + y\alpha) = F_1(x_2 + y\alpha)$ for any $x_1, x_2, y \in \text{GF}(q)$. Thus $F_1(z)$ is not a PP over $\text{GF}(q^2)$.

Now we assume that $a + b \neq 0$. Let

$$z_1 = x_1 + y_1\alpha, \quad z_2 = x_2 + y_2\alpha, \quad x_1, x_2, y_1, y_2 \in \text{GF}(q)$$

such that $F_1(z_1) = F_1(z_2)$.

By (15) and $\alpha^t \in \text{GF}(q)$, we have

$$(a - b)y_1 = (a - b)y_2, \quad (a + b)x_1 + (2y_1 + u)^t\alpha^t = (a + b)x_2 + (2y_2 + u)^t\alpha^t.$$

If $a = b$, then for any distinct $y_1, y_2 \in \text{GF}(q)$, we can obtain two elements $x_1, x_2 \in \text{GF}(q)$ with

$$(a + b)x_1 + (2y_1 + u)^t\alpha^t = (a + b)x_2 + (2y_2 + u)^t\alpha^t.$$

Thus $F_1(z)$ is not a PP over $\text{GF}(q^2)$.

If $a \neq b$, then we have $y_1 = y_2$ and $(a + b)x_1 = (a + b)x_2$, so $x_1 = x_2$. It follows that $z_1 = z_2$, which implies that $F_1(z)$ is a PP over $\text{GF}(q^2)$ if and only if $a^2 \neq b^2$.

Now we turn to prove the conclusion of the second part. By (15) and $\alpha^{t-1} \in \text{GF}(q)$, we have

$$(a + b)x_1 = (a + b)x_2, \quad (a - b)y_1 + (2y_1 + u)^t\alpha^{t-1} = (a - b)y_2 + (2y_2 + u)^t\alpha^{t-1}.$$

Hence by Theorem 2.1, $F(z)$ is a PP over $\text{GF}(q^2)$ if and only if both $(a + b)x$ and $(a - b)x + (2x + u)^t\alpha^{t-1}$ are PPs over $\text{GF}(q)$. It is easy to see that $(a - b)x + (2x + u)^t\alpha^{t-1}$ is a PP over $\text{GF}(q)$ if and only if $(a - b)x + 2x^t\alpha^{t-1}$ is a PP over $\text{GF}(q)$. The desired conclusions in the second part then follow. \square

Let q be a prime power with $q \equiv 1 \pmod{3}$. Then $3(q - 1) | q^3 - 1$, so there is an element $\alpha \in \text{GF}(q^3) \setminus \text{GF}(q)$ and $\alpha^3 \in \text{GF}(q)$. Let $\alpha^3 = b \in \text{GF}(q)$ and $\omega = \alpha^{q-1} = b^{\frac{q-1}{3}} \in \text{GF}(q)$. Then $\omega \neq 1$ and $\omega^3 = 1, 1 + \omega + \omega^2 = 0$, and $\{1, \alpha, \alpha^2\}$ is a basis of $\text{GF}(q^3)$ over $\text{GF}(q)$. Moreover, we have

$$\alpha^q = \omega\alpha, \quad \alpha^{q^2} = \omega^2\alpha.$$

Similarly, we have the following.

Theorem 29. Let q be a prime power with $q \equiv 1 \pmod{3}$ and let t be a positive integer. Let $a, b, c, u \in \text{GF}(q)$. Then

$$F(x) = ax + bx^q + cx^{q^2} + (x + x^q + x^{q^2} + u)^t$$

is a PP over $\text{GF}(q^3)$ if and only if $(a + b\omega + c\omega^2)(a + b\omega^2 + c\omega) \neq 0$ and $(a + b + c)x + 3x^t$ is a PP over $\text{GF}(q)$.

Proof. Let $x = x_1 + x_2\alpha + x_3\alpha^2$. Since $\alpha^q = \omega\alpha$ and $\alpha^{q^2} = \omega^2\alpha$, we have

$$F(x) = (a + b + c)x_1 + (a + b\omega + c\omega^2)x_2\alpha + (a + b\omega^2 + c\omega)x_3\alpha^2 + (3x_1 + u)^t.$$

By Theorem 1, $F(x)$ is a PP over $\text{GF}(q^3)$ if and only if $(a + b\omega + c\omega^2)x$, $(a + b\omega^2 + c\omega)x$ and $(a + b + c)x + (3x + u)^t$ are PPs over $\text{GF}(q)$. It is easily seen that $(a + b + c)x + (3x + u)^t$ is a PP over $\text{GF}(q)$ if and only if $(a + b + c)x + 3x^t$ is a PP over $\text{GF}(q)$. The desired conclusions then follow. \square

Let symbols and notations be the same as above. We have then the following.

Theorem 30. Let q be a prime power with $q \equiv 1 \pmod{3}$ and let t be a positive integer. Let $a, b, c, u \in \text{GF}(q)$ and define

$$F_1(x) = ax + bx^q + cx^{q^2} + (x + \omega x^q + \omega^2 x^{q^2} + u\alpha^2)^t.$$

1. When $t \not\equiv 1 \pmod{3}$, $F_1(x)$ is a PP over $\text{GF}(q^3)$ if and only if $(a + b + c)(a + b\omega + c\omega^2)(a + b\omega^2 + c\omega) \neq 0$.
2. When $t \equiv 1 \pmod{3}$, $F_1(x)$ is a PP over $\text{GF}(q^3)$ if and only if $(a + b + c)(a + b\omega^2 + c\omega) \neq 0$ and $(a + b\omega^2 + c\omega)x + \alpha^{2(t-1)}3x^t$ is a PP over $\text{GF}(q)$.

Proof. Let $x = x_1 + x_2\alpha + x_3\alpha^2$. Since $\alpha^q = \omega\alpha$ and $\alpha^{q^2} = \omega^2\alpha$, we have

$$F(x) = (a + b + c)x_1 + (a + b\omega + c\omega^2)x_2\alpha + (a + b\omega^2 + c\omega)x_3\alpha^2 + (3x_3\alpha^2 + u\alpha^2)^t.$$

Assume now that $t \not\equiv 1 \pmod{3}$. We have then $\alpha^{2t} \neq d\alpha^2$ for any $d \in \text{GF}(q)$. Let $x = x_1 + x_2\alpha + x_3\alpha^2$ and $y = y_1 + y_2\alpha + y_3\alpha^2$, $x_i, y_i \in \text{GF}(q)$, $i = 1, 2, 3$ such that $F_1(x) = F_1(y)$.

When $t \equiv 0 \pmod{3}$, we have

$$\begin{cases} (a + b\omega + c\omega^2)x_2 = (a + b\omega + c\omega^2)y_2, \\ (a + b\omega^2 + c\omega)x_3 = (a + b\omega^2 + c\omega)y_3, \\ (a + b + c)x_1 + (3x_3 + u)^t\alpha^{2t} = (a + b + c)y_1 + (3y_3 + u)^t\alpha^{2t}. \end{cases}$$

We then conclude that $x = y$ if and only if $(a + b + c)(a + b\omega + c\omega^2)(a + b\omega^2 + c\omega) \neq 0$; that is, $F_1(x)$ is a PP over $\text{GF}(q^3)$ if and only if $(a + b + c)(a + b\omega + c\omega^2)(a + b\omega^2 + c\omega) \neq 0$.

When $t \equiv 2 \pmod{3}$, we have

$$\begin{cases} (a + b + c)x_1 = (a + b + c)y_1, \\ (a + b\omega^2 + c\omega)x_3 = (a + b\omega^2 + c\omega)y_3, \\ (a + b\omega + c\omega^2)x_2 + (3x_3 + u)^t\alpha^{2t-1} = (a + b\omega + c\omega^2)y_2 + (3y_3 + u)^t\alpha^{2t-1}. \end{cases}$$

We deduce that $x = y$ if and only if $(a + b + c)(a + b\omega + c\omega^2)(a + b\omega^2 + c\omega) \neq 0$; that is, $F_1(x)$ is a PP over $\text{GF}(q^3)$ if and only if $(a + b + c)(a + b\omega + c\omega^2)(a + b\omega^2 + c\omega) \neq 0$.

When $t \equiv 1 \pmod{3}$, we have

$$\begin{cases} (a+b+c)x_1 = (a+b+c)y_1, \\ (a+b\omega+c\omega^2)x_2 = (a+b\omega+c\omega^2)y_2, \\ (a+b\omega^2+c\omega)x_3 + (3x_3+u)^t\alpha^{2t-2} = (a+b\omega^2+c\omega)y_3 + (3y_3+u)^t\alpha^{2t-2}. \end{cases}$$

By Theorem 1, $F(x)$ is a PP over $\text{GF}(q^3)$ if and only if $(a+b\omega+c\omega^2)x$, $(a+b+c)x$ and $(a+b\omega^2+c\omega)x + (3x+u)^t\alpha^{2t-2}$ are PPs over $\text{GF}(q)$; that is, $(a+b+c)(a+b\omega^2+c\omega) \neq 0$ and $(a+b\omega^2+c\omega)x + \alpha^{2(t-1)}(3x+u)^t$ is a PP over $\text{GF}(q)$. It is straightforward to see that $(a+b\omega^2+c\omega)x + \alpha^{2(t-1)}(3x+u)^t$ is a PP over $\text{GF}(q)$ if and only if $(a+b\omega^2+c\omega)x + \alpha^{2(t-1)}3x^t$ is a PP over $\text{GF}(q)$. The desired conclusion then follows. \square

9. Concluding remarks

The contributions of this paper are the four recursive constructions of permutation polynomials over $\text{GF}(q^2)$ with permutation polynomials over $\text{GF}(q)$, and the construction of permutation polynomials over $\text{GF}(2^{2m})$ with o-polynomials over $\text{GF}(2^m)$. The five generic constructions give infinitely many new permutation polynomials.

Although there are a number of references on o-polynomials, our coverage of o-polynomials in this paper contains some extensions of known families of o-polynomials. The reader is invited to settle the two conjectures on the extended families of o-polynomials.

References

- [1] A. Akbary, D. Ghioca, Q. Wang, On constructing permutations of finite fields, *Finite Fields Appl.* 17 (2011) 51–67.
- [2] X. Cao, L. Hu, Z. Zha, Constructing permutation polynomials from piecewise permutations, *Finite Fields Appl.* 26 (2014) 162–174.
- [3] C. Carlet, C. Ding and J. Yuan, Linear codes from highly nonlinear functions and their secret sharing schemes, *IEEE Trans. Inform. Theory* 51(6) (2005) 2089–2102.
- [4] W. Cherowitzo, Hyperovals in Desarguesian planes of even order, *Annals of Discrete Mathematics* 37 (1988) 87–94.
- [5] W. Cherowitzo, Hyperovals in Desarguesian planes: an update, *Discrete Math.* 155 (1996) 31–38.
- [6] W. Cherowitzo, T. Penttila, I. Pinneri, G.F. Royle, Flocks and ovals, *Geometriae Dedicata* 60 (1996) 17–37.
- [7] W. Cherowitzo, C. M. O’Keefe, and T. Penttila, A unified construction of finite geometries related to q-clans in characteristic two, *Adv. Geom.* 3 (2003) 1–21.
- [8] C. Ding and J. Yin, Signal sets from functions with optimum nonlinearity, *IEEE Trans. Communications* 55(5) (2007) 936–940.
- [9] C. Ding and J. Yuan, A family of skew Hadamard difference sets, *J. Comb. Theory Ser. A* 113 (2006) 1526–1535.
- [10] D. G. Glynn, Two new sequences of ovals in finite Desarguesian planes of even order, in: L.R.A. Casse (Ed.), *Combinatorial Mathematics X*, Lecture Notes in Mathematics 1036, Springer, 1983, pp. 217–229.
- [11] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford University Press, Oxford, 1998.
- [12] X. Hou, A new approach to permutation polynomials over finite fields, *Finite Fields Appl.* 18 (2012) 492–521.
- [13] X. Hou, Permutation polynomials over finite fields A survey of recent advances, *Finite Fields Appl.* 32 (2015) 82–119.
- [14] X. Hou, G. L. Mullen, J. A. Sellers, J. L. Yucas, Reversed Dickson polynomials over finite fields, *Finite Fields Appl.* 15 (2009) 748–773.
- [15] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, *Finite Fields Appl.* 13 (2007) 58–70.
- [16] R. Lidl, On cryptosystems based on permutation polynomials and finite fields. In T. Beth, N. Cot, and I. Ingemars-son, editors, *Advances in Cryptology - EuroCrypt-84*, volume 209 of *Lecture Notes in Computer Science*, pages 10–15, Berlin, 1985. Springer-Verlag.
- [17] R. Lidl and W. B. Muller, Permutation polynomials in RSA-cryptosystems, in: *Advances in Cryptology*, Plenum, New York, 1984, 293–301.

- [18] R. Lidl, G. L. Mullen and G. Turnwald, Dickson Polynomials, Longman Scientific Technical, Harlow, Essex, UK, 1993.
- [19] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
- [20] G. L. Mullen. Permutation polynomials and nonsingular feedback shift registers over finite fields. IEEE Trans. Information Technology, 35(4) (1989) 900–902.
- [21] C. M. O’Keefe and T. Penttila, Polynomials for hyperovals of Desarguesian plane, J. Austral. Math. Soc. (Series A) 51 (1991) 436–447.
- [22] S. E. Payne, A new infinite family of generalized quadrangles, Congressus Numerantium 49 (1985) 115–128.
- [23] J. Schwenk and K. Huber, Public key encryption and digital signatures based on permutation polynomials, Electronic Letters 34 (1998) 759–760.
- [24] R. L. Rivest, A. Shamir, and L. M. Adelman, A method for obtaining digital signatures and public-key cryptosystems, Comm. ACM 21 (1978) 120–126.
- [25] B. Segre, Sui k -archi nei piani finiti di caratteristica 2, Revue de Math. Pures Appl. 2 (1957) 289–300.
- [26] B. Segre, Ovali e curve nei piani di Galois di caratteristica due, Atti Accad. Naz. Lincei Rend. (8) 32 (1962) 785–790.
- [27] B. Segre, U. Bartocci, Ovali ed alte curve nei piani di Galois di caratteristica due, Acta Arith., 18 (1971) 423–449.
- [28] J. Sun and O. Y. Takeshita. Interleavers for turbo codes using permutation polynomials over integer rings. IEEE Trans. Information Theory, 51(1) (2005) 101–119.
- [29] Z. Tu, X. Zeng, L. Hu, Several classes of complete permutation polynomials, Finite Fields Appl. 25 (2014) 182–193.
- [30] Q. Wang, J.L. Yucas, Dickson polynomials over finite fields, Finite Fields Appl. 18 (2012) 814–831.
- [31] J. Yuan, C. Carlet and C. Ding, The weight distribution of a class of linear codes from perfect nonlinear functions, IEEE Trans. Inform. Theory 52(2) (2006) 712–717.
- [32] X. Zeng, X. Zhu, L. Hu, Two new permutation polynomials with the form $(x^{2^k} + x + \delta)^s + x$ over F_{2^n} , Appl. Algebra Eng. Commun. Comput. 21 (2010) 145–150.
- [33] Z. Zha, L. Hu and X. Cao, Constructing permutations and complete permutations over finite fields via subfield-valued polynomials, Finite Fields and Their Applications, Vol. 31, pp. 162–177, January 2015.